5G Drives New Business Models

Four revenue-generating opportunities for service provider

All In for 5G

There's a lot of buzz about 5G and the buzz is justified—perhaps even understated. To see why, you need to understand how different 5G is from its mobile technology predecessors.

Previous mobile technology upgrades delivered improvements primarily along the performance axis: 4G faster than 3G faster than 2G. In terms of business models, these generational changes primarily impacted the service provider. The rest of us—enterprises and consumers alike—benefited as our mobile phones got faster, but little else was different.

5G explodes that paradigm by delivering radical improvements in three dimensions: performance, connectivity, and latency (see figure 1). Leveraging the potential of these new capabilities, enterprises and organizations across a wide spectrum of industries and sizes can build innovative business models either working with service providers and managed service providers or with a do-it-yourself approach. In essence, 5G creates a new digital ecosystem with diverse players including cloud providers, managed security providers, enterprises, and technology partners offering services through both competition and cooperation. But these opportunities must be secured.

5G By the Numbers

1.01 Billion
5G connections by 2023, 217.2% compound annual rate (CAGR) from 2019-2023

41.6 Billion
devices estimated to be connected to the Internet by 2025

157% CAGR
growth in multi-access edge computing (MEC) adoption in wireless networks by 2024

75%
of enterprise-generated data will be created and processed at the edge by 2025

Sources: IDC, GSMA intelligence, Gartner, Frost & Sullivan

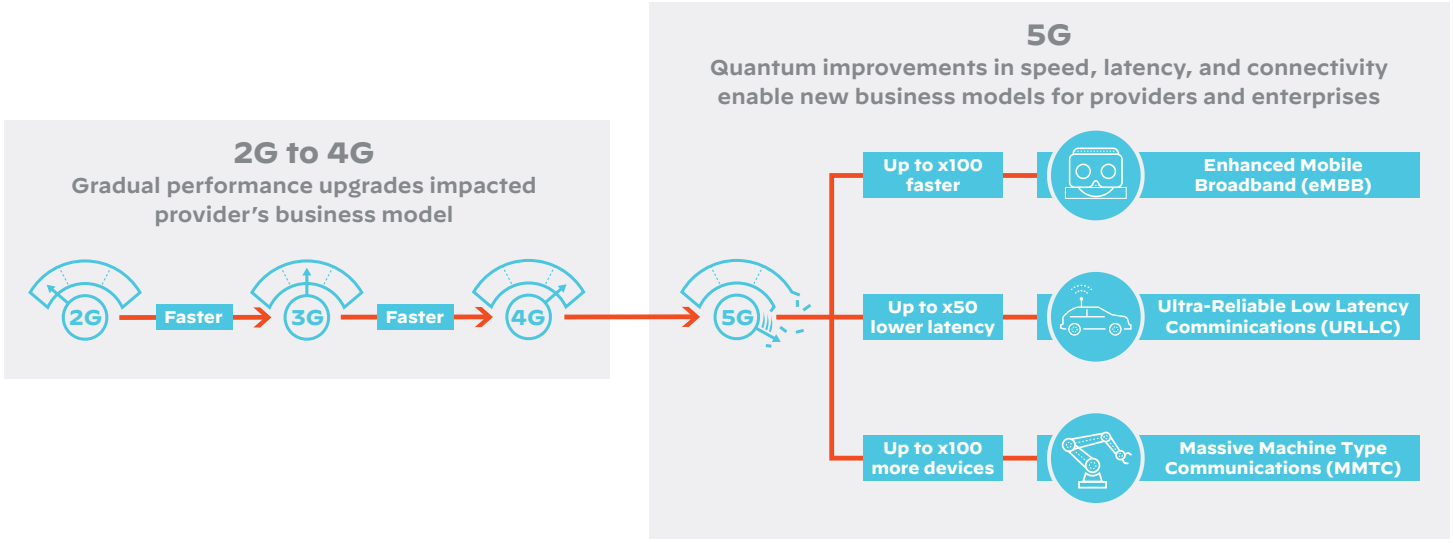

Figure 1: How 5G Improves on Previous Generations

[1] "Nutanix Enterprise Cloud Index," Nutanix, November 13, 2019.

Enterprises Embrace 5G for Digital Transformation

The new 5G capabilities offer unparalleled opportunities for businesses in more traditional industries to accelerate their digital transformation journeys. Massive connectivity and low latency in 5G drive a range of "smart" applications such as smart cities, smart homes, and smart cars. The opportunities are vast, and will rely on new ways of safeguarding 5G advances in digital transformation.

Business leaders realize the potential of 5G for their industry-specific applications and services. Adding 5G technologies to existing network architectures will not only allow businesses to modernize—it will disrupt entire industries.

On the enterprise side, 5G powers two distinct Internet of things (IoT) use cases, massive IoT and critical IoT. Massive IoT deployments employ thousands of low-cost, low-power sensors for applications such as smart cities and logistics. The focus in massive IoT is on connectivity. In contrast, critical IoT places the emphasis on reliability and low latency. Critical IoT deployments support smart grids, remote healthcare, and connected automobiles—applications where downtime can be catastrophic (see figure 2).

Healthcare

COVID-19 has shaken the healthcare world, transforming care delivery and other aspects of the business. The pandemic comes in the context of massive digitization initiatives that were already challenging enough. Going forward, 5G is poised to help care providers to enhance their telemedicine services, transmit large imaging files, use artificial intelligence to improve diagnoses, and drive the adoption of new IoT technologies such as wearables and remote monitoring equipment.

But 5G also poses additional cybersecurity risks for healthcare institutions. Hyperconnectivity expands the attack surface and gives attackers more opportunities to access and exfiltrate data. Devices such as wearables and remote sensors are difficult to secure and therefore represent vulnerabilities. In addition, critical technologies such as telesurgery rely on the low latency of 5G, making them more susceptible to even relatively minor disruptions caused by denial-of-service (DoS) and distributed DoS (DDoS0 attacks).

Retail

The cutting edge of the retail industry is data analytics, which helps organizations understand their customers better and improves in-store and online experiences. IoT-embedded sensors provide up-to-date stock levels and enable real-time communication with store employees in the dressing room and elsewhere. 5G in the hospitality sector will likely give guests more ways to customize their stay experiences. For example, it could give them control of temperatures, window shades, and lights using their mobile phones.

At the same time, the retail industry will have to take a fresh look at cybersecurity in a 5G world. For example, so-called "smart mirrors" could be hacked and expose the retailer to lawsuits for privacy violations. When stocking levels are automated using RFID sensors, hackers can enter the network via those unsecured endpoints and access personally identifiable information (PII) such as bank accounts and credit card numbers.

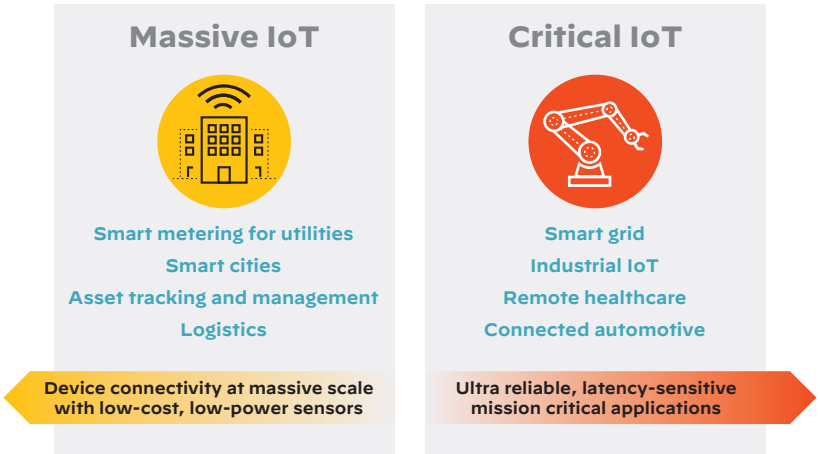

Figure 2: 5G IoT Use Cases

Financial Services

The low latency and high data capacity, and superior reliability of 5G is ready to create substantial opportunities for innovative new services. Wearables may allow institutions to better interact with their customers no matter where they are located. AI-based software can drive customized financial recommendations.

Financial institutions face the same 5G security risks as other sectors, including IoT vulnerabilities and data exfiltration. In an industry where low latency is paramount, some institutions may move critical trading applications to the edge to speed up transactions, which provides additional entry points for intruders. However, financial institutions are looking to the 5G technology to help them boost security as well. For example, banks can take advantage of the low latency and high speed of 5G networks to institute more secure biometric technologies using cloud-based verification.

Manufacturing

Many of the predictions about the smart factory will almost certainly need 5G to become reality. In 5G-enabled factories, connected devices can sense their environments and interoperate with each other, making rapid decentralized decisions that increase productivity and streamline maintenance activities. Managers will benefit from extensive amounts of real-time data generated by ubiquitous deployment of IoT sensors.

In the 5G factory, cybersecurity will have to be rethought. Hundreds or thousands of relatively unsecure sensors expand the attack surface, giving attackers more entry points. Manufacturing operations often contain sensitive process information that can be highly valuable to competitors. The high speed that 5G provides means that hackers can quickly download large amounts of intellectual property in seconds, well before the intrusion is detected.

Transportation

5G is also ready to transform the way that goods and people travel, improving safety and reliability while streamlining operations. The industry is looking to new use cases, for example, vehicle to infrastructure communications between smart vehicles and sensors located in roads and bridges to identify hazards and slow traffic flows.

Cybersecurity for 5G-enabled transportation is literally a matter of life and death, because malicious disruptions can cause deadly accidents for autonomous vehicles. In addition, interruption of transportation modalities has a significant financial impact on today's sophisticated supply chains.

Technology Enables 5G Opportunities for Providers

Service providers have opportunities to provide the support enterprises need to realize the enormous potential of 5G. Key technology enablers in 5G—such as network slicing and enterprise-grade, high reliability connectivity—pave the way for providers to offer innovative new services.

The range of opportunities for 5G revenue growth is extensive. Here we look at four prominent offerings that service providers should consider: infrastructure as a service, service as a differentiator, custom virtual networks, and edge use cases.

Opportunity 1: 5G Infrastructure as a Service

As discussed earlier, 5G represents significant opportunities for enterprises across a wide swath of industries. But how do they realize that potential? Some enterprises are planning to deploy private 5G networks, either standalone or in conjunction with public networks. In a recent survey of enterprise leaders on the forefront of adopting 5G, 43% are considering a combination of public and private 5G network slices. Another 25% are leaning toward public only, while 24% want to own and operate their 5G network outright.[1] In most cases, the mix of public and private networks will probably be influenced by enterprise requirements for control over configuration, performance, and security (see figure 3).

Figure 3: Survey results showing preferences of enterprise leaders for public versus private 5G networks (Source: Deloitte)

[1] Naima Hoque Essing and Dan Littman, "Impact of 5G Network Slicing," Deloitte Insights, August 19,2020.

However, those results can be viewed from another perspective: 75% of enterprises will look outside the organization for some or all of their 5G network services to drive digital transformation.[2] Meeting that need will take an entire 5G ecosystem, a network of diverse players including cloud providers, managed security providers, enterprises and technology partners offering services through both competition and cooperation. Key players from business and mission-critical verticals, regulatory agencies and decision makers from county governments and city councils all have a role to play in realizing the potential of 5G.

Providers occupy a pivotal position in this ecosystem because they provide the 5G core and other foundational elements of the 5G network such as mobile edge computing (MEC) and network slicing. From that vantage point, the provider becomes the locus of 5G security, a role that no other ecosystem player can match (see figure 4).

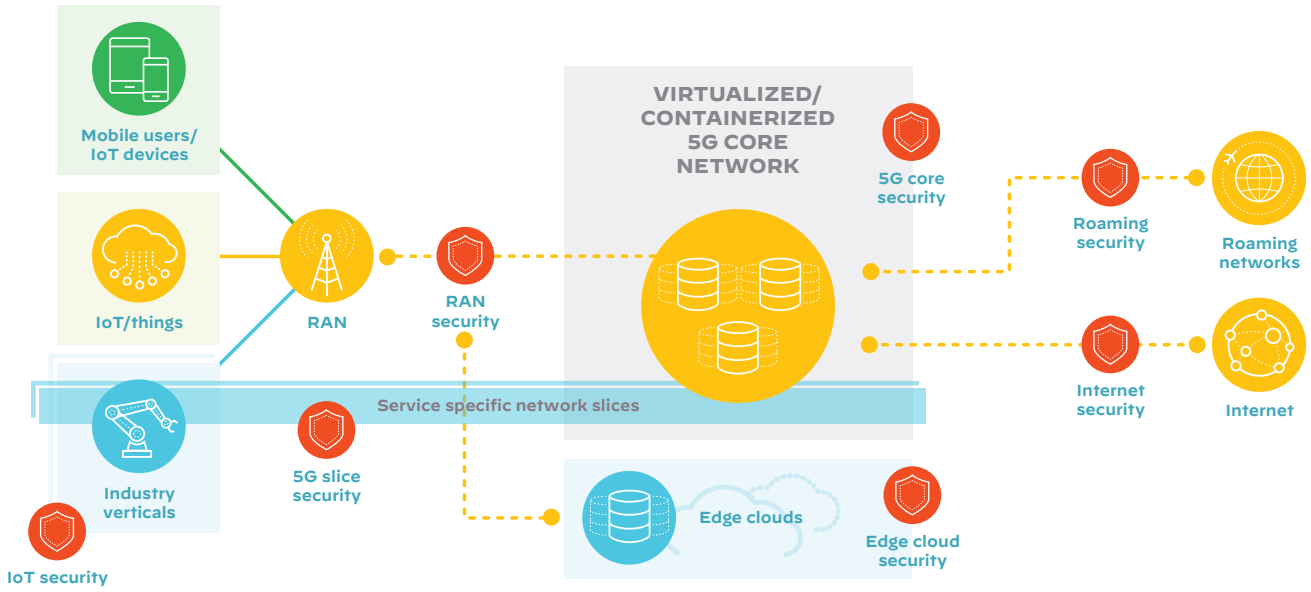

Figure 4: Security locations in the 5G architecture

[2] Ibid.

Opportunity 2: Security as a Differentiator

Public cloud providers use a shared responsibility model for security. The provider secures the infrastructure consisting of the compute, storage, database, and networking resources. The customer then must secure the upper part of the stack including operating system, applications, and data. This division is sometimes stated as the provider is responsible for security of the cloud, while the customer is responsible for security in the cloud (see figure 5).

While some enterprises have the internal expertise to secure their 5G deployments, many do not. Building that capability in-house can be expensive and a distraction from other strategic goals. The opportunity for the service provider is to offer the needed security services in the customer's area of responsibility, for example, encryption, firewall configuration, and identity and access management. Beyond the revenue-generating potential of these security-as-a-service offerings, they also offer providers a way to gain competitive advantage over providers who do not have similar offerings (figure 6).

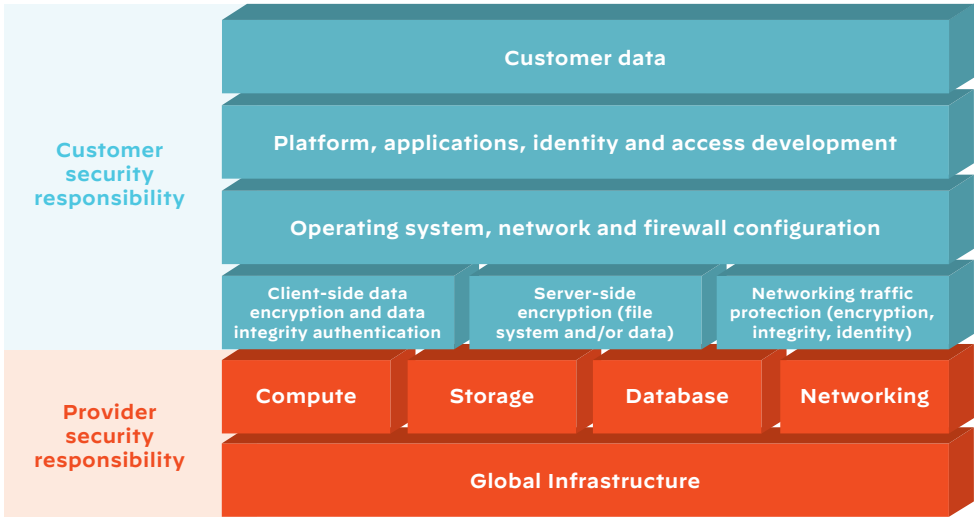

Figure 5: Shared responsibility model for cloud security

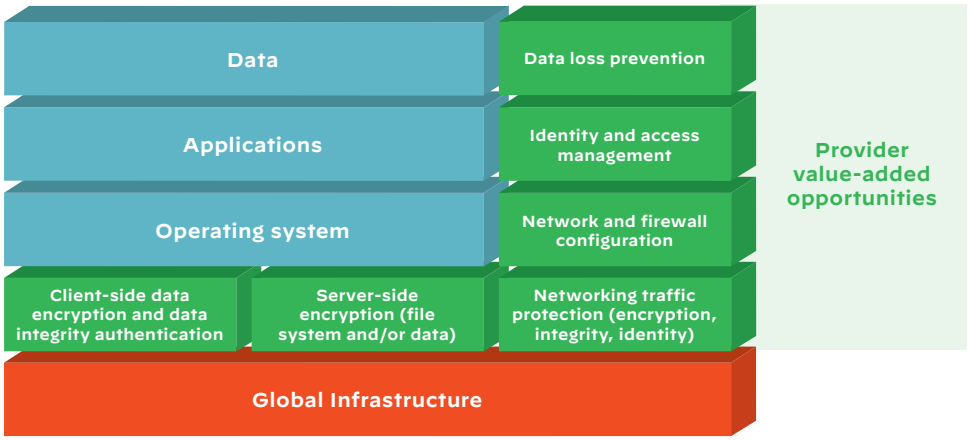

Figure 6: Security-as-a-differentiator opportunities for providers

Opportunity 3: Customized Secure Virtual Networks

As today's enterprises undergo digital transformation, they seek 5G networks security so they can confidently deploy new applications and IoT services to maximize the business value of 5G. For service providers, the fundamental business opportunity is to transform security from a checkbox requirement for selling connectivity into a revenue generator based on value-added services. They do so with new business models to monetize network functions that were previously bundled with connectivity and therefore invisible to the customer.

The key to opening up this opportunity is network slicing, which allows operators to create custom virtual networks for specific customers. For example, a manufacturing plant could require a minimum level of network performance, a utility would specify a minimum number of connections, and autonomous vehicles might focus on maximum latency.

To make this vision work, service providers and their enterprise customers will establish new trust models that place more risk on the mobile operator to meet each customer's individual requirements. Providers will likely introduce tiered billing for different services—for example, gaming requires a different billing scheme than industrial IoT (IIoT).

Along with its enormous potential, network slicing also introduces additional risks. For starters, the network slice monitor (NSM) is responsible for isolating slices from each other for security purposes. If an attacker can penetrate the NSM, every enterprise in the service provider's customer base could be compromised. Another security concern is the possibility that malicious IoT traffic can penetrate the user plane function (UPF), exposing network traffic to outside parties. Service providers who adopt network slicing must secure all these vulnerabilities and more to meet the needs of each customer (see figure 7).

Opportunity 4: Edge Deployments

As impressive as they are, the eye-catching 5G specifications can only be achieved with architectural enhancements, most notably, moving network functionality to the edge. MEC negates the latency associated with backhaul to the cloud by conducting a portion of the storage, data transfer, and computing at the network edge. This fact enables a wide variety of applications, where every millisecond counts. These opportunities include applications such as driverless vehicles, others that include the digitization of utilities such as the electric grid, and technologies like virtual reality and augmented reality. Robotics and immersive media can similarly flourish in a low-latency environment enabled by developing intelligence at the edge.

The retail industry offers a good example of how MEC can transform businesses. Brick-and-mortar retailers rely on their Wi-Fi infrastructures to connect point-of-sale (POS) devices, smart printers, digital signage, and handheld devices for in-store use. W-Fi can struggle to keep up as foot traffic, leading to sluggish performance at the very time they need to provide excellent service. Furthermore, retailers are understandable reluctant to introduce new technologies such as virtual reality when they can barely support their existing devices.

5G offers a powerful way forward for retailers. The enhanced performance of 5G over Wi-Fi boosts the responsiveness of digital devices, improving both the customer and employee experiences. In addition, retailers can adopt IoT technologies for gathering information that can help them understand customers in real time.

The revenue opportunity for providers is to launch innovative offerings that take advantage of MEC—and enable an ecosystem to flourish in business-to-business market segments. However, providers must move rapidly and invest heavily to monetize MEC before other players seize the initiative, most notably over-the-top media services, which have been siphoning revenue from service providers for years.

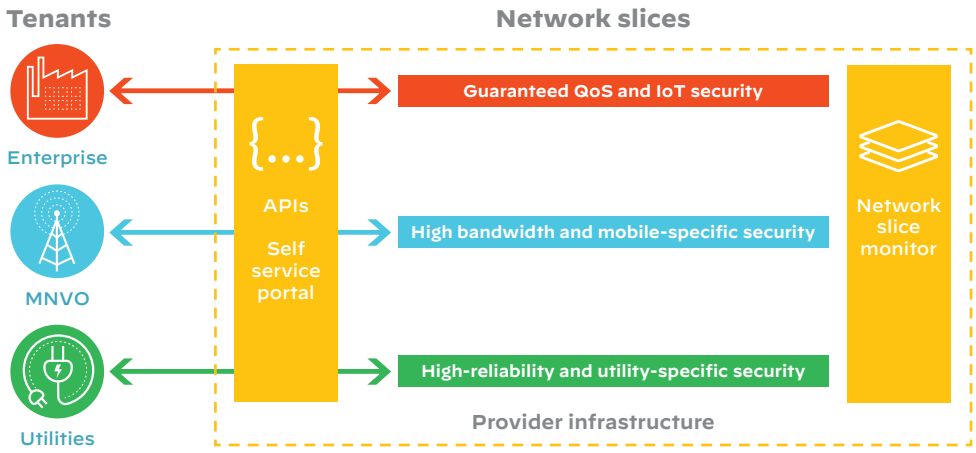

Figure 7: Security deployment in typical network slicing application

5G Vulnerabilities Increase Cybersecurity Risk

In the early stages of the 5G evolution, many stakeholders are focusing on delivering higher data speeds, latency improvements, and the overall functional redesign of mobile networks to enable greater agility, efficiency and openness. However, security cannot be forgotten. In fact, effective cybersecurity tailored for the 5G environment is an essential component for 5G success. Here are some important ways that 5G networks are more vulnerable than previous generations.[3]

Decentralization

With 5G networks comes a greater reliance on cloud and edge compute, creating a highly distributed environment that spans multi-vendor and multi-cloud infrastructures. The 5G network moves away from centralized hardware-based switching to distributed software-defined digital routing. Much of the network traffic no longer flows through a central hub, which eliminates the single hardware point where security can be deployed. As a result, security also must be decentralized to other locations such as the multi-access edge computing (MEC) (see figure 8).

Device Proliferation

The typical 5G network will host millions and millions of IoT devices for everything from public safety and military applications to healthcare and transportation use cases. Billions of IoT devices at 5G speeds translate into a much larger attack surface. The vulnerabilities of IoT devices is well known and requires a fundamentally new approach to cybersecurity for mobile telecommunications—the zero-trust approach in which no device is assumed to be secure until it has been verified.

Cloud-Native 5G Core

End-to-end stand-alone 5G networks will be software driven and cloud native. Traditional security tools and methodologies are not suited to protect the developer-driven, infrastructure-agnostic, multi-cloud patterns of cloud native applications, constantly changing at a rapid scale. Security teams require automation to secure the growing number of ever-changing microservices their organizations use.

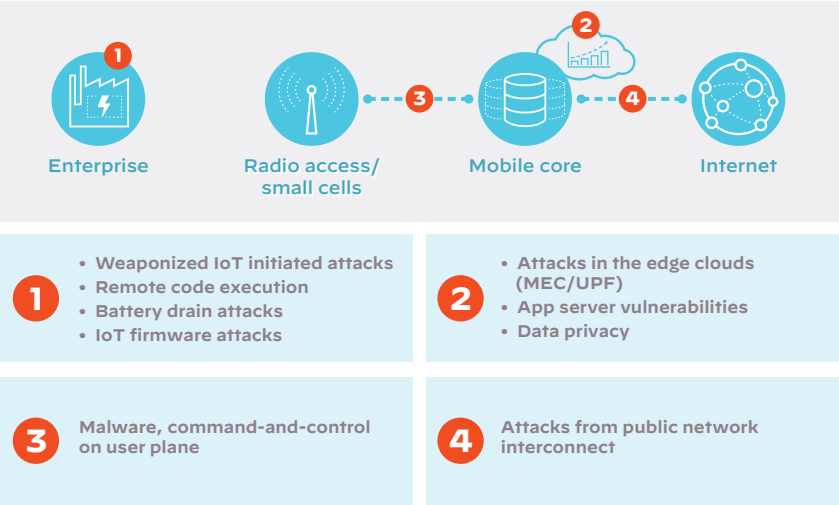

Figure 8: Typical attack points in enterprise 5G architectures

[3] Tom Wheeler and David Simpson, "Why 5G requires new approaches to cybersecurity," Brookings, September 3, 2019.

Changing Threat Landscape

The increased cost of cyber crime running into an average of more than US$17 million for organizations in industries such as financial services and utilities and energy—attackers are getting smarter.[4] Adversaries use automation for attacks and evasion. The recent solarwinds attack highlights how the attacker was trying to gain widespread, persistent access to a number of critical networks by invoking software supply chain compromise, as the most notable one in 2020. The same year, we also saw a 22.7% increase in annual cost of cybercrime.[5] New 5G use cases across industry verticals demand enterprise-grade security with the ability to gain visibility and dynamically enforce security policies at a much granular level based on parameters such as user, device and slice. The need of the hour is to ensure that any malicious activity on the network is automatically identified and immediately blocked.

More than Half of IoT Devices Vulnerable

According to the latest Unit 42 Threat Report, 57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers. 41% of attacks exploit device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses.[6]

Building a 5G Security Platform

Given the high stakes involved with 5G adoption, getting security right is of paramount importance for both provider and enterprise use cases. Organizations adopting 5G need a robust and comprehensive end-to-end security platform that encompasses all traffic (data, control and signaling planes) to protect their networks and provide a safe environment for their customers. The key elements of such a solution are zero-trust approach, deep visibility, rapid threat response, and granular policy enforcement.

Zero Trust

Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify any device that is trying to connect. Zero-trust security ensures that security is in place from untrusted domains such as supply chain, Internet, user devices, partners, and even other providers to and from within the provider's trusted domains (operator networks).[7]

Context-Driven Visibility

The distributed architecture and dynamic nature of the typical 5G network requires complete visibility across the entire network, which may consist of multiple clouds. Visibility is essential for security teams to identify infected devices and prevent device-initiated attacks before breaches can do significant damage. A 5G security platform must effectively detect and prevent threats such as signaling attacks, IoT malware, and command-and-control exploits.

Automated Threat Prevention

5G security also must include cloud-based threat intelligence for rapid responses to unknown threats and prevent attack vectors such as ransomware that cause damage in just minutes. Humans cannot react fast enough to these attacks, so automated response is an essential feature. Machine learning helps associate unknown threats with the parent malware family to further speed automated responses. Actionable insights through dynamic threat correlation help accelerate investigation of security incidents related to an enterprise or industry vertical in 5G network.

Granular Policy Enforcement

The distributed and dynamic nature of 5G architectures creates challenges in keeping policies consistent and effective. Compared to previous versions of cellular network technology standards, 5G security requires more information about network traffic, such as equipment and subscriber IDs to correlate threats on a per-slice basis.

---

[4] Floris van den Dool, "Eighth Annual Cost of Cybercrime Study," Accenture, August 14, 2020.

[5] Ibid.

[6] Marlet D. Salazar, "Palo Alto Networks study reveals 57% of IoT devices are vulnerable to high-severity attacks," Back End News, September 18, 2020.

[7] Mary K. Pratt, "What is Zero Trust? A model for more effective security," CSO Online, January 16, 2018.

Introducing Industry's First 5G-Native Security

Palo Alto Networks has introduced the industry's first 5G-native security solution, offering highly granular security for highly distributed, cloud-native 5G networks. Our solution includes containerized 5G security, real-time correlation of threats to 5G identifiers, and 5G network slice security. The Palo Alto Networks 5G security solution is supported on physical firewall appliances in the PA-7000 Series and PA-5200 Series NGFWs, VM-Series virtual next-generation firewalls (NGFWs) for virtualized 5G deployments, CN-Series container NGFWs for containerized 5G deployments. Customers using Palo Alto Networks NGFWs can continue to use the same platform to secure service provider 5G infrastructure and enterprise 5G networks.

Securing all layers of the 5G cloud stack

Compute and Infra Security

Prisma Cloud delivers cloud workload protection, providing holistic protection across hosts, containers, and serverless deployments in any cloud, throughout the application lifecycle. Reduce risk and protect the build and deploy stage of continuous integration and continuous delivery with compute and infra security.

Layer 7 Threat Protection Mobile Network Visibility

5G-Native Security offers network-based detection and protection of 5G subscribers and services. Deploy ML-driven advanced network security in your 5G infrastructure at all key locations including RAN, Roaming, Internet (Gi/SGi/N6), cellular IoT, cloud-native 5G core and edge clouds.

Security Orchestration and Automation

Cortex XSOAR orchestrates and automates your entire 5G security product stack for faster and more scalable incident response across your cloud native, hybrid and on-premises environments, resulting in up to 90% faster response times and as much as a 95% reduction in alerts requiring human intervention.

For more information about how Palo Alto Networks secures 5G networks, visit our 5G site—or sign up for a personalized demonstration and discover how we can help you secure the power of 5G.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com